A Convex Scheme for the Secrecy Capacity of a MIMO Wiretap Channel with a Single Antenna Eavesdropper

Jennifer Chakravarty, Oliver Johnson, Robert Piechocki

***Abstract*—Security has traditionally been dealt with at layers higher than the physical layer but in the wake of 5G, security at all layers is necessary to deal with the variations in complexity of connected devices. Low power devices may use physical layer security as a solution, while other devices may use physical layer security to complement security at higher layers. One key metric for physical layer security is the secrecy capacity. This is the maximum rate that a system can transmit with perfect secrecy.**

Multiple Input Multiple Output (MIMO) and Massive MIMO systems look likely to play a part in 5G, but the secrecy capacity for such systems is not fully understood. For a Gaussian MIMO channel, the secrecy capacity is a non-convex optimisation problem for which a general solution is not available. This paper presents an optimisation scheme that enables us to determine the secrecy capacity of a MIMO system with a single eavesdrop antenna. It is shown that, for certain parameters, the presented scheme is a concave problem which can therefore be solved efficiently using existing convex optimisation software.

***Keywords*—convex optimization; MIMO; secrecy capacity;**

I. INTRODUCTION

To meet ever-increasing demands for higher capacity and throughput, the launch of 5G is approaching, with aims to be commercially available by 2020 [1]. These requirements, partly fuelled by an explosion in the number of connected devices, cannot be satisfied by current communications technologies and Multiple-Input, Multiple-Output (MIMO) systems and Massive MIMO (a MIMO system with 100+ antennas at the base station) [2] are among the technologies hoped to be used for 5G [3]. In light of 5G and the reduced complexity requirements of emerging trends in technology such as low power connected Internet of Things (IoT) devices, security at physical layer has had a renewal of interest. Typically security is dealt with at higher layers than physical, but due to the stacked layers in communication devices, physical layer security may also work in tandem with higher layers. Cryptographic techniques, and other security methods, rely on generated randomness, which can be computationally heavy. Physical layer security exploits the randomness already available in the channel, typically the wireless medium, and thus is promising for low complexity devices.

Physical layer security has an information theoretic foundation and is theoretically unbreakable. Quantifying security in terms of information leakage was first considered by Shannon in [4] and the traditional model stems from Wyner's work in 1975 [5], the 'Wiretap Channel' seen in Figure 1. The typical set up considered involves two legitimate users, Alice and Bob, transmitting across a channel with an eavesdropper, Eve. The information theoretic constructs give an idea of how much useful information the eavesdropper is able to obtain, known as the information leakage. These secrecy measures, which depend on block length and the channel quality are independent of computational power and thus applicable to any technologies.

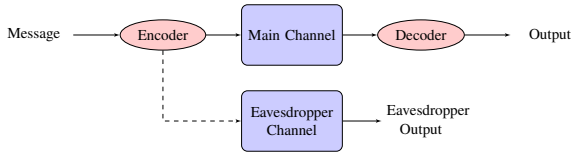

Fig. 1. The Wiretap Channel [5].

The model for communication in a MIMO system is different to that of a traditional single antenna wireless communication and thus existing security methods and physical layer methods must be adapted and explored for these systems. With multiple antennas, the users have channel matrices rather than just channel coefficients, and with these matrices come an increased number of degrees of freedom in the system design. This paper focuses on the maximum rate at which Alice may transmit to Bob reliably without Eve gaining any useful information, known as the secrecy capacity. The secrecy capacity of a channel is the theoretical maximum rate for secure, reliable communications in the presence of an eavesdropper and is formally defined below.

Definition 1.1: Consider a code with rate $R = k_m/m$ where m is the blocklength for a message of length k_m. The *secrecy capacity*, C_s, is the supremum of all rates R such that there exist sequences of codes with parameters $(m, k_m, \varepsilon_m, \delta_m)$ - where ε_m is the error threshold and δ_m is the equivocation rate - with the following properties

$$\lim_{m\to\infty} \frac{k_m}{m} \geq R$$
$$\lim_{m\to\infty} \varepsilon_m = \lim_{m\to\infty} \delta_m = 0.$$

Currently, the secrecy capacity of the MIMO channel is known to be a nonconvex optimisation problem which is difficult to solve in general. This paper presents an optimisation scheme which is convex and can be used to give the secrecy capacity and the corresponding input covariance matrix.

The structure of this paper is as follows: Section II introduces the channel setup and the previous work on secrecy capacity for MIMO systems. Section III formulates the problem addressed and states the main theorem. The proof of this theorem is presented in Section IV. Finally, Section V concludes and discusses the relevance of the result.

II. PREVIOUS WORK

A. Setup

Let n denote the number of antennas at the transmitter, n_B denote the number of antennas at the legitimate receiver and n_E the number of antennas at the eavesdropper.

The channel between the transmitter and the legitimate receiver shall be referred to as the main channel while the channel between the transmitter and the eavesdropper shall be referred to as the eavesdropper channel. Their channel matrices are described by the matrices H_B, an $n_B \times n$ matrix for the main channel and H_E, an $n_E \times n$ matrix for the eavesdropper channel. For convenience, we will define the following symmetric $n \times n$ matrices

$$K_B = (H_B^* H_B)^{\frac{1}{2}}, \tag{1}$$

$$K_E = (H_E^* H_E)^{\frac{1}{2}}. \tag{2}$$

The received vectors at Bob and Eve, denoted Y and Z respectively, are:

$$Y = H_B X + N_B,$$
$$Z = H_E Y + N_E.$$

where N_B and N_E are the noise vectors for the two channels. The input signal is subject to a power constraint P such that the trace of the covariance matrix, Q is bounded above by P. That is,

$$\operatorname{Tr} Q = \sum_{i=1}^{n} \mathbb{E}[X_i X_i^*] \leq P.$$

For the Gaussian wiretap channel the noise vectors are assumed to be Gaussian with zero mean and identity covariance:

$$N_B \sim N(0, I_{n_B}),$$
$$N_E \sim N(0, I_{n_E}).$$

The noise is independent between channel realisations. Due to the assumption of statistical independence between the antenna elements, the channel matrices H_B and H_E are modelled to have IID entries.

B. Secrecy Capacity

For the Gaussian MIMO wiretap channel, the secrecy capacity, C_s, was found in [6], [7] and independently in [8] to be of the form:

$$C_s = \max_{Q:\operatorname{Tr}(Q)\leq P} \{\log\det(I_{n_B} + H_B Q H_B^*) - \log\det(I_{n_E} + H_E Q H_E^*) \tag{3}$$

such that $Q \succeq 0$, where P is the power constraint of the system and Q is the $n \times n$ covariance matrix of the input signal.

The secrecy capacity is achieved for an input of symbols with a Gaussian distribution while using the full power available, P. The optimisation problem in Equation (3) is generally not easily solved for Q. The problem is nonconvex and the solution is only known for certain scenarios. For an overview of special cases which are known see [9]. The Multiple Input Single Output (MISO) system, where $n_B = 1$ is fully understood with the optimal Q and C_s being known in closed form determined in [6]. These results hold for any number of eavesdrop antennas. The only known case with multiple receive antennas, n_B is the '2-2-1' case, with $n = n_B = 2$ and $n_E = 1$. The optimal Q and C_s was established in [10].

Although the general maximum is not known in closed form, there is a numerical method by [11] giving an algorithm to obtain the secrecy capacity, with an associated proof of convergence to the optimum based on a matrix power series expansion.

The main work in this paper reformulates the secrecy capacity into a convex problem so that existing convex optimisation tools may be used to solve for Q. The scheme is valid for $n_B \geq n$ and $n_E = 1$, which covers a family of MIMO systems which are not yet fully understood theoretically.

III. MAIN RESULT

We first define a new optimisation problem to solve Equation (3). By [12, p73] the $\log\det(X)$ is concave for positive semidefinite matrices X. Since Q is restricted to positive semidefinite matrices, the arguments

$$I_{n_B} + H_B Q H_B^*$$

and

$$I_{n_E} + H_E Q H_E^*$$

will also be positive semidefinite and thus

$$\log\det(I_{n_B} + H_B Q H_B^*)$$

and

$$\log\det(I_{n_E} + H_E Q H_E^*)$$

are concave. However, in general, their difference is neither convex nor concave. Thus we define the following problem:

$$\max_{\operatorname{Tr}(Q)\leq P} \{\log\det(I_{n_B} + H_B Q H_B^*) - \log(s)\}, \tag{4}$$
$$\text{such that} \quad s = \det(I_{n_E} + H_E Q H_E^*)$$
$$\text{and} \quad Q \succeq 0.$$

Since $\det(M)$ is not a convex constraint for a general matrix M, this further limits the problem space to one eavesdrop antenna as this makes $I_{n_E} + H_E Q H_E^*$ a scalar. By fixing s, this becomes a concave problem. The scheme presented in this paper varies the value of s and runs convex optimisation software CVX [13] for each s. Each individual optimisation gives an output of a corresponding optimal matrix Q. Define:

$$s(Q) = \det(I_{n_E} + H_E Q H_E^*) \tag{5}$$

and

$$f(Q) = \log\det(I_{n_B} + H_B Q H_B^*) - \log s(Q). \tag{6}$$

$$\theta(s) = \max_{Q:s(Q)=s} f(Q). \tag{7}$$

A plot of $\theta(s)$ can be seen in Figure 2.

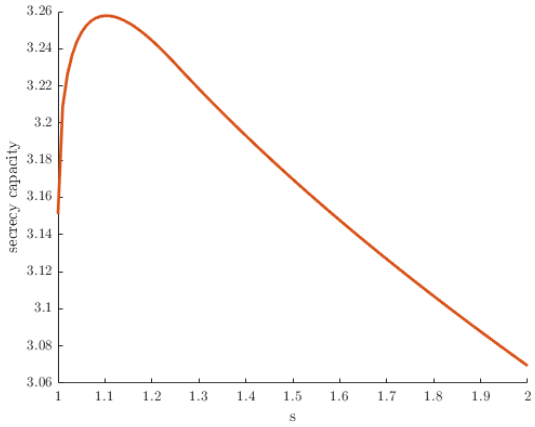

Fig. 2. $\theta(s)$ vs s for $n=2$, $n_B=3$, $n_E=1$ and $P=10$ for a particular H_B and H_E.

Finding the secrecy capacity is now a case of finding the maximum of $\theta(s)$. This is facilitated by the following Theorem, which gives a concavity result for θ which is the main result of our paper.

Let Q_i be a matrix achieving the maximum value in (7) corresponding to s_i, that is $f(Q_i)=\theta(s_i)$, for $i\in\{1,2\}$. By definition,

$$s_i = I_{n_E} + H_E Q_i H_E^*. \tag{8}$$

Without loss of generality, assume $s_1 \geq s_2$. Let s_t be a convex combination of s_1 and s_2:

$$s_t = ts_1 + (1-t)s_2$$

for $t\in[0,1]$.

Theorem 1: For $n_E=1$ and any $n_B \geq n$, then

$$\theta(s_t) \geq t\theta(s_1) + (1-t)\theta(s_2),$$

if the matrices K_B and K_E from Equations (1) and (2) satisfy

$$\frac{s_1}{\|K_B^{-1}K_E^2K_B^{-1}\|_F} - 1 \geq \max\{\lambda_{\max}(H_BQ_1H_B^*), \lambda_{\max}(H_BQ_2H_B^*)\}. \tag{9}$$

IV. PROOF OF THEOREM 1

The main argument consists of multiple steps. These can be broken down into the following:

1) Consider the problem defined in Equation (7) for a convex combination of inputs. We find a lower bound by applying new results by Courtade et al. [14].
2) Minimising the difference between the lower bound, found in Step 1, with the desired lower bound.
3) Rewrite the upper and lower bounds in terms of symmetric matrices, resulting in the conditions stated in Theorem 1.

A. Step 1

For the first step, we require the following lemma:

Lemma 1: Courtade et al. [14, Lemma 2] For positive definite matrices A, B and $t\in[0,1]$ we have that

$$\begin{aligned}&\log\det(tA+(1-t)B)\\ &\geq t\log\det(A)+(1-t)\log\det(B)\\ &\quad+\frac{t(1-t)}{2\max\{\lambda_{\max}^2(A),\lambda_{\max}^2(B)\}}\|A-B\|_F^2,\end{aligned} \tag{10}$$

where $\lambda_{\max}(\cdot)$ denotes the largest eigenvalue and $\|\cdot\|_F$ is the Frobenius norm.

For ease of notation, define

$$\mathscr{C}(A,B) = \frac{\|A-B\|_F^2}{2\max\{\lambda_{\max}^2(A),\lambda_{\max}^2(B)\}}. \tag{11}$$

The linear combination $Q_t = tQ_1+(1-t)Q_2$ satisfies the constraint $s(Q_t)=s_t$ since $n_E=1$ and

$$\begin{aligned}s_t =& t(I_{n_E}s_1 + H_EQ_2H_E^*) + (1-t)(I_{n_E}s_1 + H_EQ_2H_E^*)\\ =& I_{n_E} + H_E(tQ_1+(1-t)Q_2)H_E^*.\end{aligned}$$

Hence

$$\theta(s_t) \geq f(Q_t). \tag{12}$$

By Lemma 1, taking $A = I_{n_B} + H_BQ_1H_B^*$ and $B = I_{n_B} + H_BQ_2H_B^*$:

$$\begin{aligned}f(Q_t) =& \log\det(I_{n_B}+H_BQ_tH_B^*) - \log s_t\\ \geq& t\log\det(I_{n_B}+H_BQ_1H_B^*)\\ &+(1-t)\log\det(I_{n_B}+H_BQ_2H_B^*)\\ &-\log s_t + t(1-t)\mathscr{C}(A,B)\end{aligned} \tag{13}$$

Rewriting Equation (13) gives

$$\begin{aligned}&t\{\log\det(I_{n_B}+H_BQ_1H_B^*)-\log s_1\}\\ &+(1-t)\{\log\det(I_{n_B}+H_BQ_2H_B^*)-\log s_2\}\\ &+t(1-t)\mathscr{C}(A,B).\\ &+t\log s_1+(1-t)\log s_2-\log(ts_1+(1-t)s_2).\end{aligned}$$

By the definition of $f(\cdot)$, this can be written as

$$\begin{aligned}&tf(Q_1)+(1-t)f(Q_2)+t(1-t)\mathscr{C}(A,B)\\ &+t\log s_1+(1-t)\log s_2-\log(ts_1+(1-t)s_2).\end{aligned} \tag{14}$$

Since the Q_i are optimal matrices, this is equal to

$$\begin{aligned}&t\theta(s_1)+(1-t)\theta(s_2)+t(1-t)\mathscr{C}(A,B)\\ &+t\log s_1+(1-t)\log s_2-\log(ts_1+(1-t)s_2).\end{aligned} \tag{15}$$

B. Step 2

We aim to minimise the difference between the convex combination

$$tf(Q_1)+(1-t)f(Q_2)$$

in Equation (15) and the upper bound, $\theta(s_t)$. Thus we introduce a constant $\kappa(s_1,s_2)$ and show that:

Lemma 2: For $t \in [0,1]$,

$$t\log(s_1)+(1-t)\log(s_2)-\log(ts_1+(1-t)s_2) \geq -t(1-t)\kappa(s_1,s_2), \quad (16)$$

for

$$\kappa(s_1,s_2)=\frac{(s_1-s_2)^2}{2s_1^2} \quad (17)$$

a) Proof: Define

$$g(t) := t\log(s_1)+(1-t)\log(s_2) - \log(ts_1+(1-t)s_2)+t(1-t)\kappa(s_1,s_2). \quad (18)$$

By construction, $g(0)=g(1)=0$. To show that $g(t)\geq 0$ in the interval $t\in[0,1]$ is equivalent to showing that $g(t)$ is concave in this interval, therefore considering when $g''(t)\leq 0$. The second derivative of g is:

$$g''(t)=-2\kappa(s_1,s_2)+\frac{(s_1-s_2)^2}{s_t^2}.$$

Since $s_2 \leq s_1$, $g(t)$ is concave for the value of $\kappa(s_1,s_2)$ in Equation (17) □

C. Step 3

Combining Lemma 2 with Equation (10) means that Theorem 1 will follow from Equation (15) if

$$\frac{\|A-B\|_F^2}{2\max\{\lambda_{\max}^2(A),\lambda_{\max}^2(B)\}} \geq \kappa(s_1,s_2) \geq \frac{(s_1-s_2)^2}{2s_1^2} \quad (19)$$

where as before

$$A := I_{n_B}+H_BQ_1H_B^* \quad (20)$$

and

$$B := I_{n_B}+H_BQ_2H_B^*. \quad (21)$$

Writing $\overline{Q}:=Q_1-Q_2$ for simplicity, the Frobenius norm on the left of Equation (19) can be rewritten as

$$\begin{aligned}\|A-B\|_F^2 &= \mathrm{Tr}(H_B\overline{Q}H_B^*H_B\overline{Q}H_B^*)\\ &= \mathrm{Tr}(\overline{Q}K_B^2\overline{Q}K_B^2)\\ &= \mathrm{Tr}((K_B\overline{Q}K_B)(K_B\overline{Q}K_B))\\ &= \mathrm{Tr}(RR)=\mathrm{Tr}(RR^*)\\ &= \|R\|_F^2 \end{aligned} \quad (22)$$

where symmetric matrix

$$R := K_B\overline{Q}K_B. \quad (23)$$

Retrieving the value of $\overline{Q}$ from R requires that $H_B^*H_B$ is invertible which requires $n_B \geq n$.

Similarly, considering the numerator of the right hand side of (19) gives:

$$\begin{aligned}(s_1-s_2)^2 &= (H_E\overline{Q}H_E^*)^2\\ &= \mathrm{Tr}(\overline{Q}K_E^2\overline{Q}K_E^2)\\ &= \mathrm{Tr}((K_E\overline{Q}K_E)(K_E\overline{Q}K_E))\\ &= \mathrm{Tr}(RTRT)\\ &\leq \|RT\|_F^2 \quad (24)\\ &\leq \|R\|_F^2\|T\|_F^2. \quad (25)\end{aligned}$$

where

$$T := K_B^{-1}K_E^2K_B^{-1}. \quad (26)$$

Here Equation (24) follows by Cauchy-Schwarz, for any matrix C,

$$\mathrm{Tr}(C^2)\leq \mathrm{Tr}(C^*C)=\|C\|_F^2,$$

and Equation (25) follows by the submultiplicative property of the Frobenius norm [15, 5,6]. Therefore the inequality in Equation (19) is satisfied when

$$\frac{\|R\|_F^2\|T\|_F^2}{2s_1^2} \leq \frac{\|R\|_F^2}{2\max\{\lambda_{\max}^2(A),\lambda_{\max}^2(B)\}}. \quad (27)$$

Since each of $\lambda_{\max}^2(\cdot)$, $\|T\|_F^2$ and s_1^2 is positive, this follows by rewriting Equation (9) in the form

$$s_1 \geq \max\{\lambda_{\max}(A),\lambda_{\max}(B)\}\|T\|_F, \quad (28)$$

and the proof of Theorem 1 is complete.

V. CONCLUSIONS

Although the expression for the secrecy capacity is known for the Gaussian wiretap channel, it is not generally known how to solve the optimisation problem for the covariance matrix, Q. The method presented in this paper gives an efficient way to search for the secrecy capacity of a MIMO system and a corresponding covariance matrix for the transmission. The use of existing convex optimisation schemes makes the problem presented in Equation (3) manageable. We show that it is possible to search numerically for the maximum using linear combinations of variables.

The transmission scheme corresponding to this covariance matrix will be information theoretically secure since the user is guaranteed to be transmitting at or below the secrecy capacity.

This scheme is specific to the case with $n_E=1$ and $n_B \geq n$. This is due to the requirements which arise in the derivation of the proof. These requirements do however cover a family of MIMO systems which are not fully understood at the time of writing.

ACKNOWLEDGMENTS

This work was supported by the Engineering and Physical Sciences Research Council [grant number EP/I028153/1]; GCHQ, specifically Dene Hedges; and the University of Bristol.

REFERENCES

[1] N. Panwar, S. Sharma, and A. K. Singh, "A survey on 5G: The next generation of mobile communication," *Physical Communication*, vol. 18, pp. 64–84, 2016.

[2] F. Rusek, D. Persson, B. Lau, E. Larsson, T. Marzetta, O. Edfors, and F. Tufvesson, "Scaling up MIMO: opportunities and challenges with very large arrays," *IEEE Signal Processing Magazine*, vol. 30, no. 1, pp. 40–60, 2013.

[3] F. Jameel, M. A. A. Haider, A. A. Butt *et al.*, "Massive MIMO: A survey of recent advances, research issues and future directions," in *Recent Advances in Electrical Engineering (RAEE), 2017 International Symposium on*. IEEE, 2017, pp. 1–6.

[4] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[5] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[6] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088–3104, 2010.

[7] ——, "Secure transmission with multiple antennas – Part II: The MIMOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515–5532, Nov 2010.

[8] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4961–4972, Aug 2011.

[9] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proceedings of the National Academy of Sciences*, vol. 114, no. 1, pp. 19–26, 2017.

[10] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Transactions on Information Theory*, vol. 55, no. 9, pp. 4033–4039, Sept 2009.

[11] S. Loyka and C. D. Charalambous, "An algorithm for global maximization of secrecy rates in Gaussian MIMO wiretap channels." *IEEE Trans. Communications*, vol. 63, no. 6, pp. 2288–2299, 2015.

[12] S. Boyd and L. Vandenberghe, *Convex Optimization*. New York, NY, USA: Cambridge University Press, 2004.

[13] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 2.1," Mar. 2014. [Online]. Available: http://cvxr.com/cvx

[14] T. A. Courtade, M. Fathi, and A. Pananjady, "Wasserstein stability of the entropy power inequality for log-concave densities," 2016, arxiv:1610.07969.

[15] R. A. Horn, R. A. Horn, and C. R. Johnson, *Matrix analysis*. Cambridge university press, 1990.